

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
INFORMATION ASSOCIATED WITH
ACCOUNTS THAT ARE STORED AT
PREMISES CONTROLLED BY FACEBOOK

Case No. MJ20-167

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A-3, incorporated herein by reference.

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B-3, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. § 1958

Murder for Hire

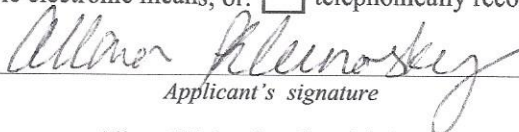
Offense Description

The application is based on these facts:

- ☒ See Affidavit of Allana Kleinosky, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.


Applicant's signature

Allana Kleinosky, Special Agent
Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 4/10/20

City and state: Seattle, Washington


Judge's signature

Brian A. Tsuchida, United States Magistrate Judge
Printed name and title

STATE OF WASHINGTON)
) SS
COUNTY OF KING)

INTRODUCTION AND AGENT BACKGROUND

2. Prior to my role as a Special Agent for the FBI, I was an Air Marshal with the Federal Air Marshal Service for three years and a Customs and Border Protection Officer with Customs and Border Protection for three and a half years. During my time as a Customs and Border Protection Officer and Federal Air Marshal, I participated in several arrests, seizures, and other law enforcement actions. I have conducted hundreds of interviews, have taken law enforcement action, and made law enforcement determinations based on the facts I gathered from these interviews.

3. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises controlled by Google LLC (“Google”), located at 1600 Amphitheater Parkway in Mountain View, California, Microsoft Corporation (“Microsoft”), located at 1 Microsoft Way in Redmond, Washington, and Facebook, Inc. (“Facebook”), located at 1601 Willow Road, Menlo Park, California (collectively, “**THE PROVIDERS**”). The information to be searched is described in the following paragraphs and in Attachments A-1, A-2, and A-3.

4. This affidavit is made in support of an application for a search warrant pursuant to Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require **THE PROVIDERS** to disclose to the government copies of the information, including the content of communications, further described in Section I of Attachments B-1, B-2, and B-3, pertaining to the following accounts:

- a. jackemerson@outlook.com (“**SUBJECT ACCOUNT 1**”)
- b. jonasmccoy@gmail.com (“**SUBJECT ACCOUNT 2**”)
- c. lluviafigueroa22@hotmail.com (“**SUBJECT ACCOUNT 3**”)
- d. lfigueroa@my.ghc.edu (“**SUBJECT ACCOUNT 4**”)
- e. kendranewman22@outlook.com (“**SUBJECT ACCOUNT 5**”)
- f. nicolestigall22@outlook.com (“**SUBJECT ACCOUNT 6**”)
- g. lluviaselene.sierrafigueroa (Facebook ID 100002531010182) (“**SUBJECT ACCOUNT 7**”)
- h. katlyn.everson.5 (“**SUBJECT ACCOUNT 8**”)
- i. cmarison (Facebook ID 28501000) (“**SUBJECT ACCOUNT 9**”)

(hereinafter, collectively the “**SUBJECT ACCOUNTS**”). Upon receipt of the information described in Section I of Attachments B-1, B-2, and B-3, government-authorized persons will review that information to locate the items described in Section II of Attachments B-1, B-2, and B-3. This warrant is requested in connection with an ongoing investigation in this district by the FBI.

5. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not

1 set forth each and every fact that I or others have learned during the course of this
2 investigation.

3 6. Based on my training and experience and the facts as set forth in this
4 affidavit, there is probable cause to believe that violations of Title 18, United States
5 Code, Sections 1958 (Murder for Hire) have been committed by LLUVIA FIGUEROA.
6 Section 1958 prohibits “us[ing] or caus[ing] another . . . to use . . . any facility of
7 interstate or foreign commerce, with intent that a murder be committed in violation of the
8 laws of any State or the United States as consideration for the receipt of, or as
9 consideration for a promise or agreement to pay, anything of pecuniary value” or
10 conspiring to do the same. There is also probable cause to search the information
11 described in Attachments A-1, A-2, and A-3, for evidence, instrumentalities, or
12 contraband of these crimes, as described in Attachments B-1, B-2, and B-3.

13 7. This warrant application is to be presented electronically pursuant to Local
14 Criminal Rule CrR 41(d)(3).

15 **BACKGROUND ON CRYPTOCURRENCY**

16 8. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to-peer,
17 network-based medium of value or exchange that may be used as a substitute for fiat
18 currency to buy goods or services or exchanged for fiat currency or other
19 cryptocurrencies. Cryptocurrency can exist digitally on the Internet, in an electronic
20 storage device, or in cloud-based servers. Although not usually stored in any physical
21 form, public and private keys (described below) used to transfer cryptocurrency from one
22 person or place to another can be printed or written on a piece of paper or other tangible
23 object. Cryptocurrency can be exchanged directly person to person, through a
24 cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is
25 not issued by any government, bank, or company; it is instead generated and controlled
26 through computer software operating on a decentralized peer-to-peer network. Most
27 cryptocurrencies have a “blockchain,” which is a distributed public ledger, run by the
28

1 decentralized network, containing an immutable and historical record of every
2 transaction.¹ Cryptocurrency is not illegal in the United States.

3 9. Bitcoin² is a type of cryptocurrency. Payments or transfers of value made
4 with bitcoins are recorded in the Bitcoin blockchain and thus are not maintained by any
5 single administrator or entity. As mentioned above, individuals can acquire bitcoins
6 through exchanges (i.e., online companies which allow individuals to purchase or sell
7 cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), Bitcoin
8 ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by
9 “mining.” An individual can “mine” bitcoins by using his/her computing power to solve
10 a complicated algorithm and verify and record payments on the blockchain. Individuals
11 are rewarded for this task by receiving newly created units of a cryptocurrency.
12 Individuals can send and receive cryptocurrencies online using many types of electronic
13 devices, including laptop computers and smart phones.

14 10. Even though the public addresses of those engaging in cryptocurrency
15 transactions are recorded on a blockchain, the identities of the individuals or entities
16 behind the public addresses are not recorded on these public ledgers. If, however, an
17 individual or entity is linked to a public address, it may be possible to determine what
18 transactions were conducted by that individual or entity. Bitcoin transactions are
19 therefore sometimes described as “pseudonymous,” meaning that they are partially
20 anonymous. And while it is not completely anonymous, Bitcoin allows users to transfer
21 funds more anonymously than would be possible through traditional banking and credit
22 systems.

23
24 _____
25 ¹ Some cryptocurrencies operate on blockchains that are not public and operate in such a way to
26 obfuscate transactions, making it difficult to trace or attribute transactions.

27 ² Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice
28 is to use “Bitcoin” (singular with an uppercase letter B) to label the protocol, software, and
community, and “bitcoin” (with a lowercase letter b) or “BTC” to label units of the
cryptocurrency. That practice is adopted here.

11. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key (or public address) is akin to a bank account number, and a private key (or private address) is akin to a Personal Identification Number (“PIN”) number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public key and the private key. A public address is represented as a case-sensitive string of letters and numbers. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address’s private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

12. Although cryptocurrencies such as Bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering, and is an oft-used means of payment for illegal goods and services on hidden services websites operating on the Tor network. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement’s efforts to track purchases within the dark web marketplaces.

13. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including: on a tangible, external device (“hardware wallet”); downloaded on a Personal Computer (“PC”) or laptop (“desktop wallet”); with an Internet-based cloud storage provider (“online wallet”); as a mobile application on a smartphone or tablet (“mobile wallet”); as printed public and private keys (“paper wallet”); and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type

1 of external or removable media device, such as a Universal Serial Bus (“USB”) thumb
2 drive or other commercially available device designed to store cryptocurrency (e.g.
3 Trezor, Keepkey, or Nano Ledger). In addition, paper wallets may contain an address
4 and a QR code³ with the public and private key embedded in the code. Paper wallet keys
5 are not stored digitally. Wallets can also be backed up into, for example, paper printouts,
6 USB drives, or CDs, and accessed through a “recovery seed” (random words strung
7 together in a phrase) or a complex password. Additional security safeguards for
8 cryptocurrency wallets can include two-factor authorization (such as a password and a
9 phrase).

10 **BACKGROUND CONCERNING THE DARK NET**

11 14. The “dark net” or “dark web” is a portion of the “Deep Web” of the
12 Internet, where individuals must use anonymizing software or applications to access
13 content and websites. Within the dark web, criminal marketplaces operate, allowing
14 individuals to buy and sell illegal items, such as drugs, firearms, and other hazardous
15 materials, with greater anonymity than is possible on the traditional Internet (sometimes
16 called the “clear web” or simply the “web”). These online market websites use a variety
17 of technologies, including the Tor network (defined below) and other encryption
18 technologies, to ensure that communications and transactions are shielded from
19 interception and monitoring. Famous dark web marketplaces, also called Hidden
20 Services, such as Silk Road, AlphaBay,⁴ and Dream Market⁵ operated similarly to clear
21 web commercial websites such as Amazon and eBay, but offered illicit goods and
22 services. There are a number of marketplaces that have appeared on the dark web that
23

24
25 ³ A QR code is a matrix barcode that is a machine-readable optical label.

26 ⁴ AlphaBay was a website on the dark web that offered drugs and other contraband for sale.
Furthermore, I know that AlphaBay was seized by U.S. law enforcement in July 2017.

27 ⁵ Dream Market was a website on the dark web that offered drugs and other contraband for sale.
28 In late March 2019, Dream Market announced it was closing on April 30, 2019 and transferring
its services to a partner company.

1 have offered contraband for sale, including narcotics. Users typically purchase narcotics
2 through these marketplaces using digital currency such as bitcoin.

3 15. “Vendors” are the dark web’s sellers of goods and services, often of an
4 illicit nature, and they do so through the creation and operation of “vendor accounts” on
5 dark web marketplaces. Customers, meanwhile, operate “customer accounts.” Vendor
6 and customer accounts are not identified by numbers, but rather monikers or “handles,”
7 much like the username one would use on a clear web site. If a moniker on a particular
8 marketplace has not already been registered by another user, vendors and customers can
9 use the same moniker across multiple marketplaces. Based on customer reviews, vendors
10 can become well known as “trusted” vendors.

11 16. The Onion Router or “Tor” network is a special network of computers on
12 the Internet, distributed around the world, that is designed to conceal the true Internet
13 Protocol (“IP”) addresses of the computers accessing the network, and thereby the
14 locations and identities of the network’s users. Tor likewise enables websites to operate
15 on the network in a way that conceals the true IP addresses of the computer servers
16 hosting the websites, which are referred to as “hidden services” on the Tor network.
17 Such “hidden services” operating on Tor have complex web addresses, which are many
18 times generated by a computer algorithm, ending in “.onion” and can only be accessed
19 through specific web browser software designed to access the Tor network. Most
20 “hidden services” are considered dark web services with no legitimate or identified
21 service provider to which legal process may be served.

22 STATEMENT OF PROBABLE CAUSE

23 **A. Summary of Investigation**

24 17. On February 12, 2020, the FBI received an anonymous tip from an
25 individual (“SOI-1”) purporting to operate a website on the dark web that offers hitmen
26 for hire. SOI-1 claimed to have received a request to murder a woman who resides in
27 Bellevue, Washington (“VICTIM”). SOI-1 stated that, although SOI-1’s website offers
28

1 to murder individuals in exchange for Bitcoin, the website is a scam, designed to steal
2 money from customers.

3 18. As described herein, the FBI has determined that, around the time of the
4 murder for hire, VICTIM's husband, J.M., had been having an extramarital affair with
5 LLUVIA FIGUEROA, a college student whom he met at a self-help course. When the
6 FBI interviewed FIGUEROA, she admitted that she paid an unknown person, located on
7 the dark web, to kill VICTIM in exchange for \$5,000 in bitcoin.

8 19. As described in further detail below, FIGUEROA and J.M. used the
9 **SUBJECT ACCOUNTS** to communicate with one another during the course of the
10 affair, and FIGUEROA used the **SUBJECT ACCOUNTS** to attempt to anonymously
11 communicate with the VICTIM, purchase bitcoin, and solicit the murder.

12 **B. Anonymous Tip**

13 20. On February 12, 2020, a complainant, SOI-1, submitted an online tip to the
14 FBI National Threat Operations Center. The tip was anonymous, sent from a ProtonMail
15 account, using an IP address associated with a Virtual Private Network ("VPN")⁶ in
16 Phoenix, Arizona. Based on my training and experience, and information gained during
17 the course of this investigation, I know that individuals often use VPNs and encrypted
18 email providers like ProtonMail in order to conceal their identities or physical locations
19 online.

20 21. In this tip, SOI-1 claimed to have information regarding a murder for hire.
21 SOI-1 claimed to be the administrator of a "dark web site that offers hitmen for hire," and
22 explained that he/she was contracted to kill VICTIM for approximately \$5,000, paid in
23

24 _____
25 ⁶ A VPN connection is a means of connecting to a private network over a public network such as
26 the Internet. A VPN is created by establishing a virtual point-to-point connection through the use
27 of dedicated connections, virtual tunneling protocols, or traffic encryption. VPNs are also
28 frequently used by people who wish to circumvent geographic IP limitations and censorship, and
to connect to proxy servers for the purpose of obfuscating the source of an internet connection or
transmission.

1 | bitcoin.⁷ SOI-1 claimed the website was set up to scam people out of money, and that no
2 | actual murders were committed by SOI-1 or anyone working on SOI-1's behalf.

3 | 22. SOI-1 explained that he/she was concerned about receiving the request to
4 | murder VICTIM, thinking that if someone was willing to pay SOI-1, that person may find
5 | other means to kill VICTIM. SOI-1 wanted to work with the FBI and police to track
6 | down the individual who had solicited the murder. SOI-1 stated "I feel that all targets
7 | that have been paid for are in danger. Customers that pay to kill someone show that they
8 | are serious about killing that person[.] I need to be in contact with you and to provide
9 | you with the target information, payments evidence, and other information to trace the
10 | customers. Customers don't give their name or details and hide their IP, but still can be
11 | tracked." SOI-1 provided information related to VICTIM and another contract, and said
12 | he/she would be willing to provide more details on additional targets.

13 | 23. SOI-1 said that when he/she had received a request to murder VICTIM, the
14 | solicitor of this murder (hereinafter referred to as the "solicitor") provided SOI-1 with
15 | VICTIM's address in Bellevue, Washington, the name of her employer, the city where
16 | she was employed, the age of her son, her routine regarding child care, and the time she
17 | returns home. The solicitor told SOI-1:

18 | Just kill her ASAP. I don't care how just make sure she's dead. I'd prefer
19 | if you shoot her in the head. She works in [corporation]⁸ in Bellevue but I
20 | don't know where exactly. I don't know if that helps you in someway. She
21 | has a 3 years old son that she picks him up at 5 P.M. so she usually gets
22 | home around 5ish. Please don't do anything to the boy. That's all.
23 | Thanks[.] Send me a proof when the job's done.

24 | 24. SOI-1 also provided a picture of VICTIM, which an FBI Special
25 | Agent Caryn Highley recognized as VICTIM, having met her in person.

26 | ⁷ SOI-1 also informed the FBI about a second murder that had been solicited on SOI-1's website
27 | unrelated to the VICTIM identified in this Affidavit. The FBI is also investigating that potential
28 | hit.

⁸ This information is redacted to protect VICTIM's privacy and safety. However, I have
determined that the corporation listed as VICTIM's employer is, in fact, accurate.

1 Additionally, SOI-1 provided the Bitcoin wallet address used for the transaction,
2 which Agent Highley confirmed on the publicly accessible blockchain received
3 approximately .53 bitcoin on February 4, 2020. Based on the value of Bitcoin on
4 that particular date, this amount is roughly equivalent to the amount that SOI-1
5 claimed he/she was paid by the solicitor—\$5,000.

6 **C. Interview of VICTIM**

7 25. On February 13, 2020, Agent Highley, along with others, interviewed
8 VICTIM and advised her of the solicitation of her murder. In order to identify who might
9 have wanted to have VICTIM killed, law enforcement asked VICTIM to identify those
10 who might have wished her harm.

11 26. VICTIM explained that, in 2010, her husband, J.M., was involved in a
12 sexual harassment lawsuit. J.M. alleged that a former employer had harassed him, which
13 led to J.M. leaving his company and suing his former boss. VICTIM felt that it was
14 unlikely that J.M.'s former employer would solicit her murder, but said it was possible
15 due to the "life altering" nature of the situation.

16 27. VICTIM explained that her husband, J.M., was involved in another lawsuit
17 after he left his former employer in October 2019 to form a business. After starting this
18 business, J.M.'s former employer sued J.M. for violation of a non-compete clause. The
19 lawsuit remains ongoing and, in November or December 2019, VICTIM paid their
20 lawyers \$5,000 for legal services from a joint account held by J.M. and VICTIM.
21 Recently, a second payment of \$5,000 had been withdrawn from her husband's business
22 account. VICTIM's husband had informed her that this second payment had been made
23 to their lawyers, since she did not have access to her husband's business account.

24 28. VICTIM also stated that, on December 23, 2019, an unknown female rang
25 VICTIM's front doorbell and asked for J.M. by name. VICTIM's Ring camera captured
26 the interaction. When VICTIM told the female that J.M. was not home, the female said
27 she was there to see VICTIM and asked to come into the house. VICTIM became
28 concerned because the female kept reaching into her pockets. The female's behavior and

her desire to enter the residence prompted VICTIM to lock the deadbolt while talking to the unknown female through the door. J.M. was not home, but utilizing the Ring camera, he joined the conversation. Shortly afterward, the female walked away. VICTIM called 911 and reported the incident to Bellevue Police Department. She also provided a copy of the video to Bellevue Police Department. VICTIM still had the video footage available. Agent Highley reviewed that video and, due to the image quality, cannot conclusively say the female is FIGUEROA, however, based on the complexion, stature, and voice, the woman in the image appears to resemble FIGUEROA.⁹ At the time, VICTIM did not believe the female knew them. The female asked for J.M. by name, but there was a package outside the residence, next to the front door that was from a family member. The package had J.M.'s full name visible on it, printed in large letters. When the female claimed to be there to see VICTIM, she referred to VICTIM as "you" and never referred to her by name.

29. VICTIM also explained that, at the end of January 2020, her employer prematurely ended a contract with a Phoenix-based company. The contract concluded due to work performance issues with this company. VICTIM communicated with an employee of this company, B.O., regularly. According to VICTIM, B.O. is familiar with VICTIM's daily routine, including the time she leaves work to pick up her son. On one occasion, B.O. traveled to Bellevue, Washington, for two weeks to work at VICTIM's employer's office. B.O. and VICTIM had several arguments due to criticism of B.O.'s work performance by VICTIM and her supervisor. B.O. has never threatened VICTIM or any other employees. Despite their turbulent relationship, VICTIM stated she would be surprised if B.O. had tried to harm her. VICTIM last spoke to B.O. on February 12, 2020. She said it was difficult to get a hold of B.O., and when she was finally able to contact B.O. on the 12th, B.O. was evasive and quickly ended the phone call.

⁹ As explained below, J.M. later explained that he recognized this person to be FIGUEROA and FIGUEROA admitted, during a proffer interview, that she was the person on camera.

30. When asked about her relationship with her husband, J.M., VICTIM said it had been strained for the last few years. She described it as a “loss of passion” and in 2018, VICTIM said her husband asked her for a divorce. She described their relationship as growing distant, turning into more of a friendship than a marriage. She said this began after her husband went to a Landmark conference. She described the conference as a self-help group designed to help people reassess their lives and make drastic changes. When her husband brought up divorce, VICTIM told her husband that she didn’t want to get a divorce. She wanted to remain a family for the sake of their son. She convinced her husband to participate in counseling. However, due to J.M.’s work schedule, he was unable to attend in-person counseling but agreed to an online counseling program. VICTIM stated she had not had an extramarital affair and did not believe her husband had either.

31. VICTIM described her and J.M.’s financial situation as strained, due to the new business and the current lawsuit. She described their financial situation as month-to-month. VICTIM stated that she and J.M. each have a \$1.5 million life insurance policy. In December 2019, J.M. began asking her to increase their life insurance policies by five hundred thousand dollars each. VICTIM did not want to meet with an insurance salesman but J.M. continued to bring it up.

D. Interview with J.M.

32. On February 13, 2020, Agent Highley, along with others, interviewed J.M. When informed about the threat, he discussed the current lawsuit involving the non-compete clause. However, he stated it was unlikely that his prior employer would make threats against him or his wife. When discussing the details contained in the threat, provided by SOI-1, he said the timeframe listed for VICTIM coming home was incorrect, as VICTIM usually comes home at a later time of night.

33. J.M. asked about VICTIM’s work with the Phoenix-based company, noting that “they would be closing that team.” He explained that VICTIM had issues with the

1 manager of the Phoenix team (believed to be B.O.) and described the Phoenix manager as
2 “snippy” and “aggressive.”

3 34. When describing his job, J.M. stated that he has “great relationships with
4 people at work,” his clients “love” him, he “just had a big win” earlier in the day, and
5 does not believe he makes enemies. He stated the “only major points of serious
6 contention are that lawsuit against me and that thing out in Phoenix.”

7 35. When asked if anything unusual had occurred recently, J.M. described the
8 incident from December 23, 2019. VICTIM notified him that someone was at the door
9 asking for him and said that an unknown female asked to enter the residence. He
10 confronted the female through the Ring camera, and was able to pull up video to see what
11 she looked like. J.M. said the female appeared to be older and seemed to be hiding her
12 face. He was unsure of the date but he believed it was after Christmas. The unknown
13 female named him, but not his wife. There was a package outside of the residence that he
14 described as having his name on it, written in large font. The unknown female reminded
15 him of an employee at his former job—the employer involved in the non-compete
16 lawsuit—but said that this employee had been living in Pennsylvania for the last two
17 years. He did not recognize her voice, he described it as having an accent, was unsure of
18 the region, and only described it as an “American” accent.¹⁰ The only other unusual
19 event he could recall was an attempted “break-in” at their residence approximately two
20 years ago.

21 36. When asked about the possibility of the suspect being someone he had a
22 relationship with, J.M. discussed the Landmark personal development course. J.M.
23 explained that he first took a course in 2018, attended a second course in 2019, and began
24 attending the third course near the end of 2019. Due to the length of the third course, he
25 dropped out at the request of his wife because there was too much going on at home.

26
27
28 ¹⁰ As described below, J.M. later recanted this explanation and told the FBI that he knew this woman was
FIGUEROA.

1 J.M. stated that he provided personal information in group discussions, but never
2 discussed information regarding his or his wife's schedule. He said he discussed issues
3 about his marriage with people in the group, but also indicated he wanted to repair the
4 marriage. J.M. said he shared the information regarding his wife with a woman, but he
5 could not remember who she was. J.M. said he couldn't imagine that she would
6 "instigate" the current situation. He stated that he didn't have any "follows" or anyone he
7 described as a "secret valentines in there or anything. You know what I mean? That I
8 knew."

9 37. During the interview, J.M. initially denied having an extramarital affair. As
10 the conversation continued, J.M. said there was "someone" at the Landmark program that
11 "really liked" him. He stated her name was LLUVIA. When asked for her last name,
12 J.M. accessed his cell phone, and he stated he last had contact with her on January 25,
13 2020, when she sent him a paper for him "to correct for school." J.M. explained that
14 LLUVIA is a student somewhere in South Bend, studying immigration law. Later during
15 the interview, J.M. accessed LLUVIA FIGUEROA's Facebook account and mentioned
16 that she was attending school at Grays Harbor College. J.M. stated that FIGUEROA sent
17 the paper to him on January 25, 2020, from her email address
18 lluviafigueroa22@hotmail.com (**SUBJECT ACCOUNT 3**). He claimed the last time
19 FIGUEROA had been in his house was June 2019.

20 38. As the conversation continued, J.M. admitted to having a sexual
21 relationship with FIGUEROA that lasted approximately "six months or so, a couple
22 times, here and there." According to J.M., the relationship started as a friendship in 2018
23 when they met at the Landmark course and later became romantic. He claimed the
24 romantic relationship ended in August 2019. J.M. said he last saw FIGUEROA in
25 January of 2020, when she told him she still loved him.

26 39. J.M. explained that, while he knew FIGUEROA, he provided her with
27 money on multiple occasions to "help her out." Most recently, on January 3, 2020,
28 FIGUEROA asked J.M. for \$5,000. J.M. said that he didn't have that amount of money

1 and instead gave her \$2,000. FIGUEROA said that the money was to help her parents
2 because they were victims of a break-in and lost their life savings. While all of the
3 previous payments were sent through Facebook, the \$2,000 payment was made through
4 J.M.'s PayPal account.

5 40. When the situation in Phoenix was brought up again, J.M. stated, "No, I
6 don't think that, I mean, if anything it's this [his relationship with FIGUEROA], this is
7 much more probabl[e] than that." When asked why he felt that way, J.M. stated it was
8 because, "[FIGUEROA] likes me and I said, I'm not gonna do that anymore..."
9 However, J.M. clarified that FIGUEROA gave him no indication of being a threat.

10 **E. Interview of FIGUEROA**

11 41. On February 14, 2020, FBI Special Agent Schroff interviewed LLUVIA
12 FIGUEROA¹¹ at her place of employment in Aberdeen, Washington. Prior to the
13 interview, Agent Schroff identified himself with his FBI credentials and asked
14 FIGUEROA if she would be willing to speak with him in a private place. Agent Schroff
15 informed FIGUEROA that she wasn't in trouble but may be a witness. FIGUEROA
16 agreed and suggested the two meet outside as there were no quiet semi-private areas
17 inside the business. Due to the temperature outside, Agent Schroff suggested the two
18 speak in his vehicle and asked FIGUEROA if she would be comfortable with that.
19 FIGUEROA agreed and the two spoke in the vehicle, with FIGUEROA sitting in the
20 passenger seat of the unlocked car. Towards the end of the interview, Agent Schroff
21 explicitly told FIGUEROA that she was not under arrest and would be going back to
22 work that night.

23 42. FIGUEROA told Agent Schroff that she participated in the Landmark
24 program, along with her brother, and met J.M. there. They became friends, and their
25 friendship evolved into a sexual relationship that has continued. FIGUEROA said that
26 she had been in J.M.'s house five to seven times, including once with her brother.

27
28 ¹¹ This interview was recorded surreptitiously.
AFFIDAVIT OF SPECIAL AGENT KLEINOSKY- 15
USAO# 2020R00187

1 FIGUEROA explained that she last saw J.M. approximately three weeks ago when they
2 went to Portland, Oregon, where they spent the night.

3 43. FIGUEROA claimed that, at first, she was unaware that J.M. was married.
4 When she found out, J.M. told FIGUEROA that his wife had cancer and that he talked to
5 his wife about divorce but decided to stay with her due to her illness. FIGUEROA stated
6 the situation made her angry. FIGUEROA initially denied hiring someone to hurt J.M.'s
7 wife.

8 44. Agent Schroff asked FIGUEROA for further details about J.M.
9 FIGUEROA explained that, even though she knew J.M. for approximately two years, she
10 did not believe she knew him completely. When asked why she felt that way,
11 FIGUEROA stated that J.M. would say things that were not accurate. For example,
12 FIGUEROA said that J.M. told her that his wife was sick, and that he could not stand his
13 wife. However, FIGUEROA observed photos online of J.M. and his wife that appeared
14 to contradict those statements. Additionally, when J.M. and FIGUEROA went to Oregon
15 together, J.M. told FIGUEROA that his wife went to Malaysia to get surgery.
16 FIGUEROA learned that VICTIM took her son with her to Malaysia, and FIGUEROA
17 thought that a sick woman would likely not travel internationally with a child.
18 FIGUEROA believed that J.M.'s son was approximately two or three years old.
19 FIGUEROA knew the three-year-old went to school in Bellevue, Washington, but she did
20 not know where.

21 45. FIGUEROA said that in November or December 2019, she "tried to send
22 [VICTIM] some images" on Facebook "about [the relationship between J.M.] and I."
23 FIGUEROA also said that, several years ago, she and her friend created a fake Facebook
24 account but claimed that she hadn't done so recently.

25 46. Although earlier in the interview FIGUEROA repeatedly denied trying to
26 murder VICTIM, as the conversation continued, FIGUEROA admitted that she solicited
27 the murder. FIGUEROA explained that "[t]he person that did that, it was me, I don't
28 know this would help right now or not, but I tried to delete it, but I couldn't do it..."

FIGUEROA said that she had used an “old phone” to solicit the hit, downloading an application on her phone to hide her identity. Based on my training and experience, and information conveyed by FIGUEROA, I believe this application is a Tor browser, used to access the dark web. FIGUEROA explained that she purchased the services of an unknown individual to kill VICTIM, and paid for those services with \$5,000 in bitcoin. FIGUEROA had previously explained that she was familiar with Bitcoin because she used it to purchase clothes from another country. FIGUEROA explained that there was an option on the website, where she had solicited the hit, to “delete” the transaction, but she was unable to do so because she could no longer access the website on her phone.

47. FIGUEROA believed there was a “fifteen-fifty” chance that the website offering hitman services was a scam. When asked how FIGUEROA felt about VICTIM being killed, she stated she was nervous. When asked if she hoping J.M. would come live with her once his wife was killed, FIGUEROA said “...yeah.” FIGUEROA denied that J.M. was involved in the plan to murder his wife. FIGUEROA said the phone she used to solicit the murder was currently at her home, in her bedroom in South Bend, Washington. She stated that she deleted her browser history on the phone and had not discussed the incident with anyone else.

48. On February 21, 2020, Agent Schroff and I tried to interview FIGUEROA again but she invoked her right to counsel and declined to be interviewed. As described herein, FIGUEROA later participated in a proffer interview on March 17, 2020.

F. VICTIM’s Facebook Account

49. I have reviewed VICTIM’s Facebook account, with her consent, and located messages sent from an account held in the name of Katlyn Everson (**SUBJECT ACCOUNT 9**). When viewing this account publicly, neither a profile picture nor a cover photo are shown for Katlyn Everson. It appeared that VICTIM had not yet accessed or opened these messages at the time that I viewed them.

50. On December 17, 2019, the Everson account sent VICTIM a series of messages. First, the Everson account sent VICTIM a photograph of J.M., followed by a

1 message that stated "I know it's none of my business but [J.M.] Im guessing your husband
2 is cheating on u. I know it because I know the person he's cheating on u with. If u dont
3 believe me, they're gonna meet up today at the Kizuki Ramen restaurant in Olympia at
4 4:30 PM. You can prove it by yourself."

5 51. On January 2, 2020, **SUBJECT ACCOUNT 9** account sent VICTIM a
6 series of pictures, which appear to show J.M. kissing and sitting next to FIGUEROA,
7 taken by what appears to be a third party at a neighboring table in the restaurant.

8 52. I showed VICTIM a copy of the photograph provided to SOI-1, when the
9 individual solicited VICTIM's murder. VICTIM confirmed that this photograph is
10 publicly accessible on VICTIM's Facebook page.

11 **G. Follow-Up Interview of J.M.**

12 53. March 3, 2020, I interviewed J.M. During this interview, I again asked him
13 about the Ring camera video, taken on December 23, 2019, when an unknown female
14 rang VICTIM's front doorbell and asked for J.M. by name. J.M. admitted that he knew
15 the woman in the video was FIGUEROA and that he had previously lied to investigators
16 when he denied recognizing the individual in the video. J.M. stated that, after this video
17 was taken, he talked to FIGUEROA and asked her why she had gone to his home.
18 FIGUEROA told J.M. that she was there to kill VICTIM and that she brought a knife
19 with her in order to accomplish the murder.

20 54. J.M. said that he had omitted this information from his prior interview
21 because he was concerned his wife would find out about the affair. J.M made the
22 following statement regarding the time frame of his relationship with FIGUEROA, which
23 he did not disclose to law enforcement during his first interview. J.M started a friendship
24 with FIGUEROA and her brother in August of 2018. J.M. stated that the relationship
25 evolved into a sexual relationship in the beginning of 2019. J.M. said he ended the
26 romantic relationship with FIGUEROA in the summer of 2019 but maintained a
27 friendship with her. J.M. stated that the relationship became romantic again in December
28

1 of 2019. J.M. stated that, the last time he saw FIGUEROA was on January 28, 2020,
2 when they met for dinner.

3 **H. FIGUEROA Proffer Interview**

4 55. On March 17, 2020, I, along with others, interviewed FIGUEROA pursuant
5 to a proffer agreement, in the presence of her counsel.

6 56. During this proffer interview FIGUEROA confirmed that she had solicited
7 VICTIM's murder. FIGUEROA explained that she had been having an affair with
8 VICTIM's husband J.M. since approximately the summer of 2018. FIGUEROA
9 explained that their relationship ebbed and flowed, with FIGUEROA ending the
10 relationship at multiple points after FIGUEROA became frustrated that J.M. would not
11 leave his wife.

12 57. FIGUEROA explained that J.M. offered several excuses for why he would
13 not leave his wife, including that his wife had cancer, he was afraid that he would lose
14 custody of his child in a divorce, and that his wife had tried to take her life when he
15 previously threatened her with divorce. FIGUEROA claimed that J.M. told her that they
16 could not be together until his wife died or something happened.

17 58. FIGUEROA stated that she and J.M. rekindled their romance for the final
18 time in the fall of 2019. After returning to her relationship with J.M., FIGUEROA took
19 several steps to try to end J.M. and VICTIM's marriage.

20 59. First, FIGUEROA tried to send VICTIM pictures of herself and J.M. being
21 intimate at a restaurant. To do this, FIGUEROA set up a fake Facebook account
22 (SUBJECT ACCOUNT 9) and sent pictures to VICTIM. These pictures were taken by
23 FIGUEROA's cousin, who was seated at a nearby table when J.M. and FIGUEROA were
24 having dinner. FIGUEROA asked her cousin to take these photographs so she could send
25 them to VICTIM. After sending these photographs, FIGUEROA received no response
26 from VICTIM.

27 60. FIGUEROA then escalated her behavior, deciding to go to VICTIM's
28 home to tell her in person about the affair. FIGUEROA and J.M. made plans to meet for

1 dinner at a restaurant in Olympia. Knowing that J.M. would be on his way to the
2 restaurant, FIGUEROA went to VICTIM's house and told VICTIM that she was looking
3 for J.M. When VICTIM said that J.M. was not home, FIGUEROA explained that she
4 had something to tell VICTIM. At that point, J.M. started speaking to FIGUEROA using
5 the Ring camera connected to VICTIM's home and FIGUEROA decided to leave.

6 61. FIGUEROA explained that, after leaving the house, FIGUEROA met J.M.
7 for dinner. J.M. asked why FIGUEROA went to his home, and FIGUEROA told him
8 that she went there to kill VICTIM. FIGUEROA stated that she did not really intend to
9 kill VICTIM, and was not armed when she went to the home, but told J.M. this because
10 she was upset. FIGUEROA claimed that J.M. wasn't angry but instead saw the behavior
11 as a sign of her dedication and affection for him.

12 62. FIGUEROA claimed that, in the past, J.M. had made comments about
13 wanting to kill his wife and once asked FIGUEROA if she knew anyone who would kill
14 his wife.

15 63. FIGUEROA confirmed that J.M. had previously sent her money using
16 Facebook messenger and recently sent her \$2,000 using PayPal. FIGUEROA explained
17 that she used this \$2,000, along with money she had saved from her college scholarship,
18 to solicit VICTIM's murder. FIGUEROA said that J.M. did not know that she planned
19 on hiring a hitman on the dark web, but believed that J.M. would be pleased if he found
20 out that she had.

21 64. FIGUEROA stated that, to solicit the murder, she used her old phone, a
22 phone that she had obtained from her pastor that was not linked to her. She then googled
23 the dark web, downloaded an application to access the dark web, and located several sites
24 offering hitmen services. FIGUEROA studied those sites, reviewing comments and
25 requesting information on pricing, before selecting her hitman. FIGUEROA explained
26 that these sites offered a multitude of services, offering to beat, maim, or kill victims, to
27 be carried out by hitmen with a range of experience levels. She selected SOI-1's site
28 because it had an escrow system, giving her a sense of security that her funds would not

1 be stolen. FIGUEROA explained that, to solicit the hit, she sent a message to SOI-1 on
2 this website, sending SOI-1 VICTIM's Facebook profile picture, VICTIM's name and
3 address, requesting that SOI-1 shoot VICTIM in the head, telling SOI-1 that she would
4 release the funds from escrow once she had a picture of the VICTIM murdered, and
5 asking SOI-1 not to harm VICTIM's child.

6 65. To obtain the \$5,000 in bitcoin necessary to pay for the hit, FIGUEROA
7 explained that she went to a number of websites that offered bitcoin wallet services.
8 FIGUEROA used fake names and email addresses on these websites, including at least
9 one email address using the domain @outlook.com. FIGUEROA said that she went to
10 multiple websites, stopping after each site asked her for identifying information or a copy
11 of her driver's license. Finally, she found a website that didn't ask her for any identifying
12 information, and FIGUEROA opened a wallet on that site using a fake email address that
13 began with the name Nicole, believed by law enforcement to be
14 nicolestigall22@outlook.com (**SUBJECT ACCOUNT 6**).

15 66. To purchase the bitcoin, FIGUEROA went to a bitcoin ATM, located
16 outside a gas station in Olympia, Washington. After FIGUEROA put cash into this ATM
17 and scanned her wallet address, bitcoin was transferred to her wallet. FIGUEROA went
18 to this ATM twice in order to obtain enough bitcoin to pay for the hit. FIGUEROA then
19 transferred this bitcoin to a wallet address provided by SOI-1.

20 67. After paying these funds, FIGUEROA claimed that weeks went by and
21 SOI-1 had still not murdered VICTIM. FIGUEROA went back to SOI-1's website and
22 asked him/her about the delay. SOI-1 told FIGUEROA that the hitman who had been
23 hired was arrested and they were going to staff another hitman to complete the hit.

24 68. In addition to contacting SOI-1, FIGUEROA explained that she also
25 contacted a second hitman, communicating with this hitman via email. FIGUEROA,
26 through her counsel, later stated that she used the email account
27 jackemerson@outlook.com (**SUBJECT ACCOUNT 7**) to communicate with that
28 hitman. FIGUEROA sent that hitman VICTIM's photograph and address but declined to

1 use that hitman's services because he/she was more expensive and less reliable than SOI-
2 1.

3 **I. THE SUBJECT ACCOUNTS**

4 69. While they were having an affair, FIGUEROA and J.M. communicated
5 using **SUBJECT ACCOUNTS 2-4**.

6 a. For example, according to information obtained from Google, on
7 August 12, 2018, J.M. used jonasmccoy@gmail.com (**SUBJECT ACCOUNT 2**)¹² to
8 send an email to FIGUEROA, using lluviafigueroa22@hotmail.com (**SUBJECT**
9 **ACCOUNT 3**).¹³

10 b. On September 28, 2018, an email was sent from
11 jonasmccoy@gmail.com (**SUBJECT ACCOUNT 2**) to lluviafigueroa22@hotmail.com
12 (**SUBJECT ACCOUNT 3**).

13 c. On October 9, 2018, jonasmccoy@gmail.com (**SUBJECT**
14 **ACCOUNT 2**) emailed FIGUEROA, using the email address lfigueroa@my.ghc.edu
15 (**SUBJECT ACCOUNT 4**).¹⁴

16 d. On November 23, 2019, lfigueroa@my.ghc.edu (**SUBJECT**
17 **ACCOUNT 4**) sent an email to jonasmccoy@gmail.com (**SUBJECT ACCOUNT 2**).

18 e. On January 24, 2020, an email was sent from
19 lluviafigueroa22@hotmail.com (**SUBJECT ACCOUNT 3**) to jonasmccoy@gmail.com
20 (**SUBJECT ACCOUNT 2**).

21 f. On February 9, 2020, an email was sent from
22 jonasmccoy@gmail.com (**SUBJECT ACCOUNT 2**) to lluviafigueroa22@hotmail.com
23 (**SUBJECT ACCOUNT 3**).

24
25
26 ¹² According to Google, the email account jonasmccoy@gmail.com (**SUBJECT ACCOUNT 2**) was registered in
the name of J.M. on February 3, 2006.

27 ¹³ According to Microsoft, the email address lluviafigueroa22@hotmail.com (**SUBJECT ACCOUNT 3**) was
registered in the name of LLUVIA FIGUEROA on August 5, 2017.

28 ¹⁴ FIGUEROA is a student at Grays Harbor Community College. As described herein, this account is serviced by
Microsoft.

1 70. During the time period of the affair, J.M. and FIGUEROA also used
2 **SUBJECT ACCOUNTS 7 and 9** on Facebook to communicate and so that J.M. could
3 send money to FIGUEROA.

4 a. FIGUEROA used the account lluviaselene.sierrafigueroa
5 (Facebook ID 100002531010182) (**SUBJECT ACCOUNT 7**). According to
6 Facebook, this account was registered in the name of LLUVIA FIGUEROA on
7 May 23, 2011.

8 b. J.M. used the account cmarison (Facebook ID 28501000)
9 (**SUBJECT ACCOUNT 9**). According to Facebook, this account was registered
10 in the name of J.M. on December 5, 2004.

11 c. From September 2018 through August 2019, FIGUEROA,
12 using **SUBJECT ACCOUNT 7**, exchanged messages with J.M., using
13 **SUBJECT ACCOUNT 9**, on Facebook. Both also had payment information
14 registered to their accounts.

15 71. FIGUEROA also used a variety of fake accounts to communicate with
16 VICTIM and/or further her plot to murder VICTIM.

17 a. FIGUEROA used the Facebook account katlyn.everson.5
18 (**SUBJECT ACCOUNT 8**) to send VICTIM intimate photographs of her and J.M.
19 at a restaurant and to alert VICTIM to the affair. FIGUEROA explained that she
20 created this **SUBJECT ACCOUNT 8** so she could anonymously communicate
21 with VICTIM.

22 b. FIGUEROA also stated that she created fake email accounts
23 in furtherance of her crimes. The FBI searched FIGUEROA's phone, pursuant to
24 a warrant, and located two accounts—kendranewman22@outlook.com
25 (**SUBJECT ACCOUNT 5**) and nicolestigall22@outlook.com (**SUBJECT**
26 **ACCOUNT 6**) listed in the phone. According to information obtained from
27 Microsoft, **SUBJECT ACCOUNT 5** was registered in the name of "Kendra
28 Newman" on May 3, 2019. **SUBJECT ACCOUNT 6** was registered in the name

1 of “Nicole Stigall” on April 28, 2019. According to IP login history for these
2 accounts, both were logged into on March 17, 2020 (the day of FIGUEROA’s
3 proffer) using the IP address 98.237.218.5. FIGUEROA has also used that IP
4 address to log into **SUBJECT ACCOUNTS 3 and 8**. According to publicly
5 accessible search engines, this IP address geolocates to Comcast Communications
6 in Aberdeen, Washington, near where FIGUEROA resides.

7 c. According to information obtained from Microsoft, it appears
8 that FIGUEROA used **SUBJECT ACCOUNT 5** to communicate with Facebook
9 regarding **SUBJECT ACCOUNT 8**. For example, on March 8, 2020, Facebook
10 sent **SUBJECT ACCOUNT 5** an email, directed to the user “Katlyn Everson.”

11 d. According to information obtained from Microsoft, it appears
12 that FIGUEROA used **SUBJECT ACCOUNT 6** to communicate with
13 cryptocurrency companies. For example, according to information obtained from
14 Microsoft, on January 13, 2020, **SUBJECT ACCOUNT 6** sent an email to
15 support@coinmama.com, a cryptocurrency exchange platform that enables users
16 to buy or sell bitcoin using a credit card, debit card, or bank transfer.

17 e. Finally, according to FIGUEROA, she used the email account
18 jackemerson@outlook.com (**SUBJECT ACCOUNT 1**) to communicate with the
19 second hitman who did she decided not to hire after providing him/her with
20 VICTIM’s identifying information. According to Microsoft, **SUBJECT**
21 **ACCOUNT 1** was registered in the name of “Jack Emerson” in the United
22 Kingdom on October 31, 2016 and has been accessed using an IP address that
23 geolocates to the United Kingdom. This email account has a number of emails
24 stored in it, including those sent from BB gun sites, video game sites, and
25 cryptocurrency sites. It is believed that this email address belongs to the hitman
26 that FIGUEROA discussed, but declined to, hire.

27 72. In order to gather information related to FIGUEROA’s efforts to
28 solicit VICTIM’s murder, including evidence that FIGUEROA was having an

1 | affair with J.M., FIGUEROA accepted money from J.M., FIGUEROA used a fake
2 | account to communicate with VICTIM, FIGUEROA purchased cryptocurrency in
3 | order to pay for the hit, and FIGUEROA communicated with another hitman
4 | during this time period, I request authorization to search the **SUBJECT**
5 | **ACCOUNTS.**

6 | **BACKGROUND CONCERNING ONLINE ACCOUNTS**

7 | 73. As explained herein, information stored in connection with an online
8 | account may provide crucial evidence of the “who, what, why, when, where, and how” of
9 | the criminal conduct under investigation, thus enabling the United States to establish and
10 | prove each element or alternatively, to exclude the innocent from further suspicion.

11 | 74. In my training and experience, the information stored in connection with an
12 | online account can indicate who has used or controlled the account. This “user
13 | attribution” evidence is analogous to the search for “indicia of occupancy” while
14 | executing a search warrant at a residence. For example, email communications, contacts
15 | lists, and images sent (and the data associated with the foregoing, such as date and time)
16 | may indicate who used or controlled the account at a relevant time.

17 | 75. Further, information maintained by the email provider can show how and
18 | when the account was accessed or used. For example, as described below, email
19 | providers typically log the Internet Protocol (IP) addresses from which users access the
20 | email account, along with the time and date of that access. By determining the physical
21 | location associated with the logged IP addresses, investigators can understand the
22 | chronological and geographic context of the email account access and use relating to the
23 | crime under investigation. This geographic and timeline information may tend to either
24 | inculcate or exculpate the account owner. Additionally, information stored at the user’s
25 | account may further indicate the geographic location of the account user at a particular
26 | time (e.g., location information integrated into an image or video sent via email).

27 | 76. Stored electronic data may provide relevant insight into the email account
28 | owner’s state of mind as it relates to the offense under investigation. For example,

information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

1. Google's Services

77. In my training and experience, I have learned that Google provides a variety of online services, including electronic mail ("email") access and instant messaging (otherwise known as "chat" messaging), to the general public. Google provides subscribers email and chat accounts at the domain name "@gmail.com." Google also allows subscribers to register a custom domain name and set up Google services such as chat and email using that domain name instead of "@gmail.com."

A. Subscriber Records and Account Content

78. Subscribers obtain an account by registering with Google. When doing so, email providers like Google ask the subscriber to provide certain personal identifying information. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users, and to help establish who has dominion and control over the account.¹⁵

79. Email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's websites), and other log files that reflect

¹⁵ The relevance of the evidence in Google's possession to the present investigation, applies with equal force to the evidence in the possession of Microsoft. For the sake of brevity, the explanation of this relevance will not be fully repeated with respect to Microsoft below.

1 usage of the account. In addition, email providers often have records of the IP address
2 used to register the account and the IP addresses associated with particular logins to the
3 account. Because every device that connects to the Internet must use an IP address, IP
4 address information can help to identify which computers or other devices were used to
5 access the email account.

6 80. In some cases, email account users will communicate directly with an email
7 service provider about issues relating to the account, such as technical problems, billing
8 inquiries, or complaints from other users. Email providers typically retain records about
9 such communications, including records of contacts between the user and the provider's
10 support services, as well records of any actions taken by the provider or user as a result of
11 the communications. In my training and experience, such information may constitute
12 evidence of the crimes under investigation because the information can be used to
13 identify the account's user or users.

14 81. In general, an email that is sent to a Google subscriber is stored in the
15 subscriber's "mail box" on Google's servers until the subscriber deletes the email. When
16 the subscriber sends an email, it is initiated at the user's computer, transferred via the
17 Internet to Google servers, and then transmitted to its end destination. Google often
18 maintains a copy of received and sent emails. Unless the sender specifically deletes an
19 email from the Google server, the email can remain on the system indefinitely. Even if
20 the subscriber deletes the email, it may continue to be available on Google's servers for
21 some period of time.

22 82. A sent or received email typically includes the content of the message,
23 source and destination addresses, the date and time at which the email was sent, and the
24 size and length of the email. If an email user writes a draft message but does not send it,
25 that message may also be saved by Google but may not include all of these categories of
26 data.

27 83. In addition to email and chat, Google offers subscribers numerous other
28 services including: Android, Blogger, Google Alerts, Google Calendar, Google Chrome

1 Sync, Google Cloud Print, G-Suite, Google Developers Console, Google Drive, Google
 2 Hangouts, Google Maps, Google Payments, Google Photos, Google Search Console,
 3 Google Voice, Google+, Google Profile, Location History, Web & Activity, Search, and
 4 YouTube, among others. Thus, a subscriber to a Google account can also store files,
 5 including address books, contact lists, calendar data, photographs and other files, on
 6 servers maintained and/or owned by Google. For example, Google Calendar is a
 7 calendar service that users may utilize to organize their schedule and share events with
 8 others. Google Drive may be used to store data and documents, including spreadsheets,
 9 written documents (such as Word or Word Perfect) and other documents. Google Photos
 10 can be used to create photo albums, store photographs, and share photographs with others
 11 and “You Tube,” allows users to view, store and share videos. Google Search Console
 12 records a Google account user’s search queries. And Google Web & Activity records
 13 certain browsing history depending on whether the account holder is logged into their
 14 account. Like many internet service companies (including the companies discussed
 15 below), the services Google offers are constantly changing and evolving.

16 **2. Microsoft’s Services**

17 84. Microsoft is an internet service provider that offers a variety of online
 18 services including email accounts (Outlook.com or Hotmail), cloud computing
 19 (Microsoft OneDrive, Office and Office365), gaming services (Xbox), video
 20 conferencing (Skype), web browsing and search tools (Bing Search, Microsoft Edge, and
 21 Internet Explorer), maps, an online marketplace (Microsoft Store), and other services.
 22 Microsoft also provides remote computing services for devices that use Windows
 23 operating systems, including security services and parental control services which collect
 24 information about the use of the devices (e.g., internet browsing history, software usage
 25 history, and other information).

26 85. A Microsoft account (formerly known as a Windows Live account) is what
 27 Microsoft customers may use to sign into Microsoft services such as Outlook.com (or
 28 Hotmail), Office, OneDrive, Skype, Xbox, Windows, and more. A user may create a

1 Microsoft account with any email address (Microsoft accounts are not limited to those
2 who use Microsoft email accounts) and a password and thereafter use that email address
3 and password to sign in to any Microsoft program or service.

4 86. According to online databases, Microsoft services the domain @
5 my.ghc.edu, on behalf of Grays Harbor Community College.

6 87. In my training and experience email providers like Microsoft typically
7 retain certain transactional information about the creation and use of each account on
8 their systems. This information can include the date on which the account was created,
9 the length of service, records of log-in (*i.e.*, session) times and durations, the types of
10 service utilized, the status of the account (including whether the account is inactive or
11 closed), the methods used to connect to the account (such as logging into the account via
12 a website), and other log files that reflect usage of the account. In addition, email
13 providers often have records of the IP address used to register the account and the IP
14 addresses associated with particular logins to the account. Because every device that
15 connects to the Internet must use an IP address, IP address information can help to
16 identify which computers or other devices were used to access the email account, which
17 can help establish the individual or individuals who had dominion and control over the
18 account

19 88. In general, an email that is sent to a Microsoft subscriber is stored in the
20 subscriber's "mail box" on Microsoft's servers until the subscriber deletes the email. If
21 the subscriber does not delete the message, the message can remain on Microsoft's
22 servers indefinitely. Even if the subscriber deletes the email, it may continue to be
23 available on Microsoft's servers for a certain period of time.

24 89. When the subscriber sends an email, it is initiated at the user's computer,
25 transferred via the Internet to Microsoft's servers, and then transmitted to its end
26 destination. Microsoft often maintains a copy of the email sent. Unless the sender of the
27 email specifically deletes the email from Microsoft's server, the email can remain on the
28

1 system indefinitely. Even if the sender deletes the email, it may continue to be available
2 on Microsoft's servers for a certain period of time.

3 90. A sent or received email typically includes the content of the message,
4 source and destination addresses, the date and time at which the email was sent, and the
5 size and length of the email. If an email user writes a draft message but does not send it,
6 that message may also be saved by Microsoft but may not include all of these categories
7 of data.

8 91. Microsoft provides a variety of online, or "cloud," services in addition to
9 email access, to the public and to customers who utilize Hotmail accounts that are served
10 by Microsoft. Microsoft's various cloud services are associated with a single Microsoft
11 account, which is typically associated with a Microsoft email address, but can be
12 associated with any email address. The various cloud services provided by Microsoft are
13 optional and can be turned "on" or "off" by the user.

14 92. In providing services such as Outlook, OneDrive, Xbox, calendar services,
15 online file storage, storage of browsing history, storage of search history, and locations
16 history, Microsoft collects information that constitute evidence of the crimes under
17 investigation. For example, such evidence can be used to discover or confirm the identity
18 and location users of the service at a particular time.

19 **c. Facebook's Services**

20 93. Facebook owns and operates a free-access social networking website of the
21 same name that can be accessed at <http://www.facebook.com>. Facebook allows its users
22 to establish accounts with Facebook, and users can then use their accounts to share
23 written news, photographs, videos, and other information with other Facebook users, and
24 sometimes with the general public.

25 94. Facebook asks users to provide basic contact and personal identifying
26 information to Facebook, either during the registration process or thereafter. This
27 information may include the user's full name, birth date, gender, contact e-mail
28 addresses, Facebook passwords, physical address (including city, state, and zip code),

1 telephone numbers, screen names, websites, and other personal identifiers. Facebook
2 also assigns a user identification number to each account.

3 95. Facebook users may join one or more groups or networks to connect and
4 interact with other users who are members of the same group or network. Facebook
5 assigns a group identification number to each group. A Facebook user can also connect
6 directly with individual Facebook users by sending each user a "Friend Request." If the
7 recipient of a "Friend Request" accepts the request, then the two users will become
8 "Friends" for purposes of Facebook and can exchange communications or view
9 information about each other. Each Facebook user's account includes a list of that user's
10 "Friends" and a "News Feed," which highlights information about the user's "Friends,"
11 such as profile changes, upcoming events, and birthdays.

12 96. Facebook users can select different levels of privacy for the
13 communications and information associated with their Facebook accounts. By adjusting
14 these privacy settings, a Facebook user can make information available only to himself or
15 herself, to particular Facebook users, or to anyone with access to the Internet, including
16 people who are not Facebook users. A Facebook user can also create "lists" of Facebook
17 friends to facilitate the application of these privacy settings. Facebook accounts also
18 include other account settings that users can adjust to control, for example, the types of
19 notifications they receive from Facebook.

20 97. Facebook users can create profiles that include photographs, lists of
21 personal interests, and other information. Facebook users can also post "status" updates
22 about their whereabouts and actions, as well as links to videos, photographs, articles, and
23 other items available elsewhere on the Internet. Facebook users can also post information
24 about upcoming "events," such as social occasions, by listing the event's time, location,
25 host, and guest list. In addition, Facebook users can "check in" to particular locations or
26 add their geographic locations to their Facebook posts, thereby revealing their geographic
27 locations at particular dates and times. A particular user's profile page also includes a
28 "Wall," which is a space where the user and his or her "Friends" can post messages,

1 attachments, and links that will typically be visible to anyone who can view the user's
2 profile.

3 98. Facebook allows users to upload photos and videos, which may include any
4 metadata such as location that the user transmitted when s/he uploaded the photo or
5 video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a
6 photo or video. When a user is tagged in a photo or video, he or she receives a
7 notification of the tag and a link to see the photo or video. For Facebook's purposes, the
8 photos and videos associated with a user's account will include all photos and videos
9 uploaded by that user that have not been deleted, as well as all photos and videos
10 uploaded by any user that have that user tagged in them.

11 99. Facebook users can exchange private messages on Facebook with other
12 users. Those messages are stored by Facebook unless deleted by the user. Facebook
13 users can also post comments on the Facebook profiles of other users or on their own
14 profiles; such comments are typically associated with a specific posting or item on the
15 profile. In addition, Facebook has a chat feature that allows users to send and receive
16 instant messages through Facebook Messenger. These chat communications are stored in
17 the chat history for the account. Facebook also has Video and Voice Calling features,
18 and although Facebook does not record the calls themselves, it does keep records of the
19 date of each call.

20 100. If a Facebook user does not want to interact with another user on Facebook,
21 the first user can "block" the second user from seeing his or her account.

22 101. Facebook has a "like" feature that allows users to give positive feedback or
23 connect to particular pages. Facebook users can "like" Facebook posts or updates, as
24 well as webpages or content on third-party (i.e., non-Facebook) websites. Facebook
25 users can also become "fans" of particular Facebook pages.

26 102. Facebook has a search function that enables its users to search Facebook for
27 keywords, usernames, or pages, among other things.

1 103. Each Facebook account has an activity log, which is a list of the user's
2 posts and other Facebook activities from the inception of the account to the present. The
3 activity log includes stories and photos that the user has been tagged in, as well as
4 connections made through the account, such as "liking" a Facebook page or adding
5 someone as a friend. The activity log is visible to the user but cannot be viewed by
6 people who visit the user's Facebook page.

7 104. Facebook also has a Marketplace feature, which allows users to post free
8 classified ads. Users can post items for sale, housing, jobs, and other items on the
9 Marketplace.

10 105. In addition to the applications described above, Facebook also provides its
11 users with access to thousands of other applications ("apps") on the Facebook platform.
12 When a Facebook user accesses or uses one of these applications, an update about that
13 the user's access or use of that application may appear on the user's profile page.

14 106. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP
15 address. These logs may contain information about the actions taken by the user ID or IP
16 address on Facebook, including information about the type of action, the date and time of
17 the action, and the user ID and IP address associated with the action. For example, if a
18 user views a Facebook profile, that user's IP log would reflect the fact that the user
19 viewed the profile, and would show when and from what IP address the user did so.

20 107. Social networking providers like Facebook typically retain additional
21 information about their users' accounts, such as information about the length of service
22 (including start date), the types of service utilized, and the means and source of any
23 payments associated with the service (including any credit card or bank account number).
24 In some cases, Facebook users may communicate directly with Facebook about issues
25 relating to their accounts, such as technical problems, billing inquiries, or complaints
26 from other users. Social networking providers like Facebook typically retain records
27 about such communications, including records of contacts between the user and the
28

1 provider's support services, as well as records of any actions taken by the provider or
2 user as a result of the communications.

3 108. As explained herein, information stored in connection with a Facebook
4 account may provide crucial evidence of the "who, what, why, when, where, and how" of
5 the criminal conduct under investigation, thus enabling the United States to establish and
6 prove each element or alternatively, to exclude the innocent from further suspicion. In
7 my training and experience, a Facebook user's IP log, stored electronic communications,
8 and other data retained by Facebook, can indicate who has used or controlled the
9 Facebook account. This "user attribution" evidence is analogous to the search for
10 "indicia of occupancy" while executing a search warrant at a residence. For example,
11 profile contact information, private messaging logs, status updates, and tagged photos
12 (and the data associated with the foregoing, such as date and time) may be evidence of
13 who used or controlled the Facebook account at a relevant time. Further, Facebook
14 account activity can show how and when the account was accessed or used. For
15 example, as described herein, Facebook logs the Internet Protocol (IP) addresses from
16 which users access their accounts along with the time and date. By determining the
17 physical location associated with the logged IP addresses, investigators can understand
18 the chronological and geographic context of the account access and use relating to the
19 crime under investigation. Such information allows investigators to understand the
20 geographic and chronological context of Facebook access, use, and events relating to the
21 crime under investigation. Additionally, Facebook builds geo-location into some of its
22 services. Geo-location allows, for example, users to "tag" their location in posts and
23 Facebook "friends" to locate each other. This geographic and timeline information may
24 tend to either inculcate or exculpate the Facebook account owner. Last, Facebook
25 account activity may provide relevant insight into the Facebook account owner's state of
26 mind as it relates to the offense under investigation. For example, information on the
27 Facebook account may indicate the owner's motive and intent to commit a crime (e.g.,
28

1 information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting
2 account information in an effort to conceal evidence from law enforcement).

3 109. Therefore, the computers of Facebook are likely to contain all the material
4 described above, including stored electronic communications and information concerning
5 subscribers and their use of Facebook, such as account access information, transaction
6 information, and other account information.

7 **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

8 110. Pursuant to Title 18, United States Code, Section 2703(g), this application
9 and affidavit for a search warrant seeks authorization to require **THE PROVIDERS**, and
10 their agents and employees, to assist agents in the execution of this warrant. Once issued,
11 the search warrant will be presented to **THE PROVIDERS** with direction that they
12 identify the accounts described in Attachments A-1, A-2, and A-3 to this affidavit, as
13 well as other subscriber and log records associated with the accounts, as set forth in
14 Section I of Attachments B-1, B-2, and B-3 to this affidavit.

15 111. The search warrant will direct **THE PROVIDERS** to create an exact copy
16 of the specified account and records.

17 112. I, and/or other law enforcement personnel will thereafter review the copy of
18 the electronically stored data and identify from among that content those items that come
19 within the items identified in Section II to Attachments B-1, B-2, and B-3 for seizure.

20 113. Analyzing the data contained in the forensic copy may require special
21 technical skills, equipment, and software. It could also be very time-consuming.
22 Searching by keywords, for example, can yield thousands of “hits,” each of which must
23 then be reviewed in context by the examiner to determine whether the data is within the
24 scope of the warrant. Merely finding a relevant “hit” does not end the review process.
25 Keywords used originally need to be modified continuously, based on interim results.
26 Certain file formats, moreover, do not lend themselves to keyword searches, as keywords,
27 search text, and many common email, database and spreadsheet applications do not store
28 data as searchable text. The data may be saved, instead, in proprietary non-text format.


1 And, as the volume of storage allotted by service providers increases, the time it takes to
2 properly analyze recovered data increases, as well. Consistent with the foregoing,
3 searching the recovered data for the information subject to seizure pursuant to this
4 warrant may require a range of data analysis techniques and may take weeks or even
5 months. All forensic analysis of the data will employ only those search protocols and
6 methodologies reasonably designed to identify and seize the items identified in Section II
7 of Attachments B-1, B-2, and B-3 to the warrant.

8 114. Based on my experience and training, and the experience and training of
9 other agents with whom I have communicated, it is necessary to review and seize a
10 variety of e-mail communications, chat logs and documents, that identify any users of the
11 subject account and e-mails sent or received in temporal proximity to incriminating e-
12 mails that provide context to the incriminating communications.


13 CONCLUSION

14 115. Based on the forgoing, I respectfully request that the Court issue the
15 proposed search warrant. This Court has jurisdiction to issue the requested warrant
16 because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18
17 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of
18 the United States . . . that - has jurisdiction over the offense being investigated.” 18
19 U.S.C. § 2711(3)(A)(i). Additionally, for information sought from Microsoft, the Court
20 “is in . . . a district in which the provider . . . is located or in which the wire or electronic
21 communications, records, or other information are stored.” 18 U.S.C. § 2711(3)(A)(ii).
22 Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not
23 required for the service or execution of this warrant.

1 116. Accordingly, by this Affidavit and Warrant I seek authority for the
2 government to search all of the items specified in Section I, Attachments B-1, B-2, and
3 B-3 (attached hereto and incorporated by reference herein) to the Warrant, and
4 specifically to seize all of the data, documents and records that are identified in Section II
5 to that same Attachment.

6
7 
8 Allana Kleinosky, Affiant
9 Special Agent

10 The above-named agent provided a sworn statement attesting to the truth of the
11 foregoing affidavit on the 10 day of April, 2020.

12 
13
14 HONORABLE BRIAN A. TSUCHIDA
15 United States Magistrate Judge
16
17
18
19
20
21
22
23
24
25
26
27
28

ATTACHMENT A-1

Google Accounts to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with Google account:

jonasmccoy@gmail.com (SUBJECT ACCOUNT 2)

(the "Account") that are stored at a premises controlled by Google, LLC, a company that accepts service of legal process at 1600 Amphitheatre Parkway in Mountain View, California.

ATTACHMENT B-1**Particular Things to be Seized****I. Information to be disclosed by Google, LLC:**

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of Google, LLC (“Google”), including any data, messages, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under Title 18, United States Code, Section 2703(f), Google is required to disclose the following information to the government for each Account or identifier listed in Attachment A-1, from June 1, 2018 to the present:

- a. All electronic mail content and/or preserved data (including email, attachments, and embedded files);
- b. All subscriber records associated with the specified account, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as IP address, media access card addresses, or any other unique device identifiers recorded by Google in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;
- c. all contact lists;
- d. all account history, including any records of communications between Google and any other person about issues relating to the accounts, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider’s support services, as well as records of any actions taken by the provider or subscriber in connection with the service.

Google is hereby ordered to disclose the above information to the government within **14 days** of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Section 1958 (Murder for Hire), those violations occurring between June 2018 and the present, for each of the Accounts listed on Attachment A-1, including the following:

a. any information related to FIGUEROA, including communications with or about FIGUEROA, plans to meet FIGUEROA, and photographs of FIGUEROA;

b. any information related to J.M.'s relationship with FIGUEROA, including a romantic relationship with FIGUEROA;

c. any information related to J.M.'s relationship with VICTIM, including communications regarding divorce, separation, or illness, or evidence that J.M. was unhappy in his marriage or sought to murder VICTIM;

d. any information related to a plan to solicit murder, including by accessing websites or contacting individuals to solicit murder;

e. any information related to J.M.'s or FIGUEROA's attendance at a Landmark course or FIGUEROA's attempts to visit or actual visits to VICTIM's house;

f. any information related to payments made by J.M. to FIGUEROA;

g. any information related to FIGUEROA's transfer, purchase, sale, or disposition of Bitcoin or other cryptocurrency;

h. any information related to J.M.'s or FIGUEROA's assets, including their bank records, checks, credit card bills, account information, and other financial records, to include life insurance policies.

i. any information related to use of the dark web, including use or downloading of a Tor browser;

1 j. any information related to J.M.'s statements to FIGUEROA
2 regarding VICTIM;

3 k. any information related to efforts to delete browsing history or
4 undertake other acts to remain anonymous online, including by accessing VPNs or
5 creating multiple email accounts in a short time frame;

6 l. any information consisting of, referring to, or reflecting use of
7 cryptocurrency, including cryptocurrency client software, cryptocurrency wallet files, and
8 related private encryption keys, seed phrases, or other passwords;

9 m. any information consisting of, referring to, or reflecting use of
10 encryption or digital signature software, such as PGP encryption, and related public and
11 private encryption keys;

12 n. any information related to cryptocurrency applications and wallets,
13 to include information regarding current account balance and transaction history, *i.e.*,
14 date, time, amount, an address of the sender/recipient of a cryptocurrency transaction
15 maintained in such wallets;

16 o. any information reflecting cryptocurrencies, including web history,
17 and documents showing the location, source, and timing of acquisition of any
18 cryptocurrencies, to include wallets, wallet addresses, and seed phrases; and

19 p. Evidence that serves to identify any person who uses or accesses the
20 Account or who exercises in any way any dominion or control over the Account;

21 q. Evidence that may identify the aliases names, online user names,
22 "handles" and/or "nics" of those who exercise in any way any dominion or control over
23 the specified Accounts as well as records or information that may reveal the true
24 identities of these individuals;

25 r. Other log records, including IP address captures, associated with the
26 specified Accounts;

27 s. Subscriber records associated with the specified Account, including
28 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session

1 times and durations; 4) length of service (including start date) and types of services
2 utilized; 5) telephone or instrument number or other subscriber number or identity,
3 Including any temporarily assigned network address such as IP address, media access
4 card addresses, or any other unique device identifiers recorded by internet service
5 provider in relation to the account; 6) account log files (login IP address, account
6 activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means
7 and source of payment; and 9) lists of all related accounts;

8 t. Records of communications between the internet service provider
9 and any person purporting to be the account holder about issues relating to the Account,
10 such as technical problems, billing inquiries, or complaints from other users about the
11 specified Account. This to include records of contacts between the subscriber and the
12 provider's support services, as well as records of any actions taken by the provider or
13 subscriber as a result of the communications.

14 u. Information identifying accounts that are linked or associated with
15 the Account.

16
17 This warrant authorizes a review of electronically stored information,
18 communications, other records and information disclosed pursuant to this warrant in
19 order to locate evidence, fruits, and instrumentalities described in this warrant. The
20 review of this electronic data may be conducted by any government personnel assisting in
21 the investigation, who may include, in addition to law enforcement officers and agents,
22 attorneys for the government, attorney support staff, and technical experts. Pursuant to
23 this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the
24 custody and control of attorneys for the government and their support staff for their
25 independent review.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT
TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by
the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the
information contained in this certification is true and correct. I am employed by
_____, and my title is _____. I am
qualified to authenticate the records attached hereto because I am familiar with how the
records were created, managed, stored, and retrieved. I state that the records attached
hereto are true duplicates of the original records in the custody of _____.

The attached records consist of _____ [GENERALLY DESCRIBE
RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time
of the occurrence of the matter set forth by, or from information transmitted by, a person
with knowledge of those matters, they were kept in the ordinary course of the regularly
conducted business activity of _____, and they were made by
_____ as a regular practice; and

b. such records were generated by _____'s electronic
process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or
file(s) in the custody of _____ in a manner to ensure that they are true
duplicates of the original records; and

2. the process or system is regularly verified by _____, and at
all times pertinent to the records certified here the process and system functioned
properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of
the Federal Rules of Evidence.

Date Signature

AFFIDAVIT OF SPECIAL AGENT KLEINOSKY- 43
USAO# 2020R00187

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-2

Microsoft Accounts to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with Microsoft accounts:

jackemerson@outlook.com (**SUBJECT ACCOUNT 1**)

lluviafigueroa22@hotmail.com (**SUBJECT ACCOUNT 3**)

lfigueroa@my.ghc.edu (**SUBJECT ACCOUNT 4**)

kendranewman22@outlook.com (**SUBJECT ACCOUNT 5**)

nicolestigall22@outlook.com (**SUBJECT ACCOUNT 6**)

(the “Accounts”) that are stored at a premises controlled by Microsoft Corporation, a company that accepts service of legal process at 1 Microsoft Way in Redmond, Washington.

ATTACHMENT B-2**Particular Things to be Seized****I. Information to be disclosed by Microsoft Corporation:**

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of Microsoft Corporation ("Microsoft"), including any data, messages, records, files, logs, or information that has been deleted but is still available to Microsoft, or has been preserved pursuant to a request made under Title 18, United States Code, Section 2703(f), Microsoft is required to disclose the following information to the government for each account or identifier listed in Attachment A-2, from June 2018 to the present:

- a. All electronic mail content and/or preserved data (including email, attachments, and embedded files);
- b. All subscriber records associated with the specified account, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as IP address, media access card addresses, or any other unique device identifiers recorded by Microsoft in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;
- c. all contact lists;
- d. any Microsoft Chat/Messenger information and/or records, including any Microsoft Chat/Messenger Friends list, time, date, and IP address logs for Chat and Messenger use, and any archived web messenger communications stored on Microsoft servers;
- e. any Microsoft Notepad information and/or records;
- f. any Microsoft Calendar information and/or records,

g. any Microsoft Groups information and/or records including member lists, e-mail addresses of members, messages, files, calendars, database content, and photographs;

h. any stored documents;

i. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

j. The types of service utilized;

k. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

l. All account history, including any records of communications between Microsoft and any other person about issues relating to the accounts, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber in connection with the service.

Microsoft is hereby ordered to disclose the above information to the government within **14 days** of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Section 1958

1 (Murder for Hire), those violations occurring between June 2018 and the present, for each
2 of the Accounts listed on Attachment A-2, including the following:

3 a. any information related to J.M.'s relationship with FIGUEROA,
4 including communications between the two, plans to meet, and photographs of
5 FIGUEROA and J.M. (together or held by or sent to the other);

6 b. any information related to romantic feelings between J.M. and
7 FIGUEROA, desire to remain a couple, or desire to break up or end their affair;

8 c. any information related to FIGUEROA's desire to have J.M. end his
9 marriage or to marry or solely be romantically involved with FIGUEROA.

10 d. any information related to J.M.'s relationship with VICTIM,
11 including communications regarding divorce, separation, or illness, or evidence that J.M.
12 was unhappy in his marriage or sought to murder VICTIM;

13 e. any information related to a plan to solicit murder, including by
14 accessing websites or contacting individuals to solicit murder;

15 f. any information related to J.M.'s or FIGUEROA's attendance at a
16 Landmark course or FIGUEROA's attempts to visit or actual visits to VICTIM's house;

17 g. any information related to payments made by J.M. to FIGUEROA;

18 h. any information related to FIGUEROA's transfer, purchase, sale, or
19 disposition of Bitcoin or other cryptocurrency;

20 i. any information related to J.M.'s or FIGUEROA's assets, including
21 their bank records, checks, credit card bills, account information, and other financial
22 records, to include life insurance policies.

23 j. any information related to use of the dark web, including use or
24 downloading of a Tor browser;

25 k. any information related to J.M.'s statements to FIGUEROA
26 regarding VICTIM;

1 l. any information related to efforts to delete browsing history or
2 undertake other acts to remain anonymous online, including by accessing VPNs or
3 creating multiple email accounts in a short time frame;

4 m. any information related to the creation of a fake Facebook account to
5 contact VICTIM or fake email accounts to use in furtherance of the solicitation for
6 murder;

7 n. any information related to prior attempts to harm or threaten
8 VICTIM, or to reveal J.M.'s and FIGUEROA's affair;

9 o. any information consisting of, referring to, or reflecting use of
10 cryptocurrency, including cryptocurrency client software, cryptocurrency wallet files, and
11 related private encryption keys, seed phrases, or other passwords;

12 p. any information consisting of, referring to, or reflecting use of
13 encryption or digital signature software, such as PGP encryption, and related public and
14 private encryption keys;

15 q. any information related to cryptocurrency applications and wallets,
16 to include information regarding current account balance and transaction history, *i.e.*,
17 date, time, amount, an address of the sender/recipient of a cryptocurrency transaction
18 maintained in such wallets;

19 r. any information reflecting cryptocurrencies, including web history,
20 and documents showing the location, source, and timing of acquisition of any
21 cryptocurrencies, to include wallets, wallet addresses, and seed phrases; and

22 s. Evidence that serves to identify any person who uses or accesses the
23 Accounts or who exercises in any way any dominion or control over the Accounts;

24 t. Evidence that may identify the aliases names, online user names,
25 "handles" and/or "nics" of those who exercise in any way any dominion or control over
26 the specified Accounts as well as records or information that may reveal the true
27 identities of these individuals;

1 u. Other log records, including IP address captures, associated with the
2 specified Accounts;

3 v. Subscriber records associated with the specified Accounts, including
4 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session
5 times and durations; 4) length of service (including start date) and types of services
6 utilized; 5) telephone or instrument number or other subscriber number or identity,
7 Including any temporarily assigned network address such as IP address, media access
8 card addresses, or any other unique device identifiers recorded by internet service
9 provider in relation to the account; 6) account log files (login IP address, account
10 activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means
11 and source of payment; and 9) lists of all related accounts;

12 w. Records of communications between the internet service provider
13 and any person purporting to be the account holder about issues relating to the Accounts,
14 such as technical problems, billing inquiries, or complaints from other users about the
15 specified Accounts. This to include records of contacts between the subscriber and the
16 provider's support services, as well as records of any actions taken by the provider or
17 subscriber as a result of the communications.

18 x. Information identifying accounts that are linked or associated with
19 the Accounts.

20 This warrant authorizes a review of electronically stored information,
21 communications, other records and information disclosed pursuant to this warrant in
22 order to locate evidence, fruits, and instrumentalities described in this warrant. The
23 review of this electronic data may be conducted by any government personnel assisting in
24 the investigation, who may include, in addition to law enforcement officers and agents,
25 attorneys for the government, attorney support staff, and technical experts. Pursuant to
26 this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the
27 custody and control of attorneys for the government and their support staff for their
28 independent review.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT
TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by _____, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of _____.

The attached records consist of _____ [GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of _____, and they were made by _____ as a regular practice; and

b. such records were generated by _____'s electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of _____ in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by _____, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date _____ Signature _____

AFFIDAVIT OF SPECIAL AGENT KLEINOSKY- 50
USAO# 2020R00187

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-3

Facebook Accounts to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with Facebook accounts:

lluviaselene.sierrafigueroa (Facebook ID 100002531010182)

(SUBJECT ACCOUNT 7)

katlyn.everson.5 **(SUBJECT ACCOUNT 8)**

cmarison (Facebook ID 28501000) **(SUBJECT ACCOUNT 9)**

(the “Accounts”) that are stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered at 1601 Willow Road in Menlo Park, California.

ATTACHMENT B-3**Particular Things to be Seized****I. Information to be disclosed by Facebook, Inc.:**

To the extent that the information described in Attachment A-3 is within the possession, custody, or control of Facebook, Inc. ("Facebook"), including any data, messages, records, files, logs, or information that has been deleted but is still available to Facebook, or has been preserved pursuant to a request made under Title 18, United States Code, Section 2703(f), Facebook is required to disclose the following information to the government for each account or identifier listed in Attachment A-3, from June 2018 to the present:

a. All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

b. All activity logs for the account and all other documents showing the user's posts and other Facebook activities;

c. All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;

d. All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

e. All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the

1 hardware model, operating system version, unique device identifiers, mobile network
2 information, and user agent string;

3 f. All other records and contents of communications and messages made or
4 received by the user, including all Messenger activity, private messages, chat history,
5 video and voice calling history, and pending “Friend” requests;

6 g. All “check ins” and other location information;

7 h. All IP logs, including all records of the IP addresses that logged into the
8 account;

9 i. All records of the account’s usage of the “Like” feature, including all
10 Facebook posts and all non-Facebook webpages and content that the user has “liked”;

11 j. All information about the Facebook pages that the account is or was a “fan”
12 of;

13 k. All past and present lists of friends created by the account;

14 l. All records of Facebook searches performed by the account;

15 m. All information about the user’s access and use of Facebook Marketplace;

16 n. The types of service utilized by the user;

17 o. The length of service (including start date) and the means and source of any
18 payments associated with the service (including any credit card or bank account number);

19 p. All privacy settings and other account settings, including privacy settings
20 for individual Facebook posts and activities, and all records showing which Facebook
21 users have been blocked by the account;

22 q. All records pertaining to communications between Facebook and any
23 person regarding the user or the user’s Facebook account, including contacts with support
24 services and records of actions taken;

25 r. **All Facebook payment data**, including funds sent or received by the user.

26 Facebook is hereby ordered to disclose the above information to the government
27 within **14 days** of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Section 1958 (Murder for Hire), those violations occurring between June 2018 and the present, for each of the Accounts listed on Attachment A-3, including the following:

a. any information related to J.M.'s relationship with FIGUEROA, including communications between the two, plans to meet, and photographs of FIGUEROA and J.M. (together or held by or sent to the other);

b. any information related to romantic feelings between J.M. and FIGUEROA, desire to remain a couple, or desire to break up or end their affair;

c. any information related to FIGUEROA's desire to have J.M. end his marriage or to marry or solely be romantically involved with FIGUEROA.

d. any information related to J.M.'s relationship with VICTIM, including communications regarding divorce, separation, or illness, or evidence that J.M. was unhappy in his marriage or sought to murder VICTIM;

e. any information related to a plan to solicit murder, including by accessing websites or contacting individuals to solicit murder;

f. any information related to J.M.'s or FIGUEROA's attendance at a Landmark course or FIGUEROA's attempts to visit or actual visits to VICTIM's house;

g. any information related to payments made by J.M. to FIGUEROA;

h. any information related to FIGUEROA's transfer, purchase, sale, or disposition of Bitcoin or other cryptocurrency;

i. any information related to J.M.'s or FIGUEROA's assets, including their bank records, checks, credit card bills, account information, and other financial records, to include life insurance policies.

j. any information related to use of the dark web, including use or downloading of a Tor browser;

1 k. any information related to J.M.'s statements to FIGUEROA
2 regarding VICTIM;

3 l. any information related to efforts to delete browsing history or
4 undertake other acts to remain anonymous online, including by accessing VPNs or
5 creating multiple email accounts in a short time frame;

6 m. any information related to the creation of a fake Facebook account to
7 contact VICTIM or fake email accounts to use in furtherance of the solicitation for
8 murder;

9 n. any information related to prior attempts to harm or threaten
10 VICTIM, or to reveal J.M.'s and FIGUEROA's affair;

11 o. any information consisting of, referring to, or reflecting use of
12 cryptocurrency, including cryptocurrency client software, cryptocurrency wallet files, and
13 related private encryption keys, seed phrases, or other passwords;

14 p. any information consisting of, referring to, or reflecting use of
15 encryption or digital signature software, such as PGP encryption, and related public and
16 private encryption keys;

17 q. any information related to cryptocurrency applications and wallets,
18 to include information regarding current account balance and transaction history, *i.e.*,
19 date, time, amount, an address of the sender/recipient of a cryptocurrency transaction
20 maintained in such wallets;

21 r. any information reflecting cryptocurrencies, including web history,
22 and documents showing the location, source, and timing of acquisition of any
23 cryptocurrencies, to include wallets, wallet addresses, and seed phrases; and

24 s. Evidence that serves to identify any person who uses or accesses the
25 Accounts or who exercises in any way any dominion or control over the Accounts;

26 t. Evidence that may identify the aliases names, online user names,
27 "handles" and/or "nics" of those who exercise in any way any dominion or control over
28

1 the specified Accounts as well as records or information that may reveal the true
2 identities of these individuals;

3 u. Other log records, including IP address captures, associated with the
4 specified Accounts;

5 v. Subscriber records associated with the specified Accounts, including
6 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session
7 times and durations; 4) length of service (including start date) and types of services
8 utilized; 5) telephone or instrument number or other subscriber number or identity,
9 Including any temporarily assigned network address such as IP address, media access
10 card addresses, or any other unique device identifiers recorded by internet service
11 provider in relation to the account; 6) account log files (login IP address, account
12 activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means
13 and source of payment; and 9) lists of all related accounts;

14 w. Records of communications between the internet service provider
15 and any person purporting to be the account holder about issues relating to the Accounts,
16 such as technical problems, billing inquiries, or complaints from other users about the
17 specified Accounts. This to include records of contacts between the subscriber and the
18 provider's support services, as well as records of any actions taken by the provider or
19 subscriber as a result of the communications.

20 x. Information identifying accounts that are linked or associated with
21 the Accounts.

22
23 This warrant authorizes a review of electronically stored information,
24 communications, other records and information disclosed pursuant to this warrant in
25 order to locate evidence, fruits, and instrumentalities described in this warrant. The
26 review of this electronic data may be conducted by any government personnel assisting in
27 the investigation, who may include, in addition to law enforcement officers and agents,
28 attorneys for the government, attorney support staff, and technical experts. Pursuant to

1 | this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the
2 | custody and control of attorneys for the government and their support staff for their
3 | independent review.
4 |
5 |
6 |
7 |
8 |
9 |
10 |
11 |
12 |
13 |
14 |
15 |
16 |
17 |
18 |
19 |
20 |
21 |
22 |
23 |
24 |
25 |
26 |
27 |
28 |

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT
TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by
the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the
information contained in this certification is true and correct. I am employed by
_____, and my title is _____. I am
qualified to authenticate the records attached hereto because I am familiar with how the
records were created, managed, stored, and retrieved. I state that the records attached
hereto are true duplicates of the original records in the custody of _____.

The attached records consist of _____ [GENERALLY DESCRIBE
RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time
of the occurrence of the matter set forth by, or from information transmitted by, a person
with knowledge of those matters, they were kept in the ordinary course of the regularly
conducted business activity of _____, and they were made by
_____ as a regular practice; and

b. such records were generated by _____'s electronic
process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or
file(s) in the custody of _____ in a manner to ensure that they are true
duplicates of the original records; and

2. the process or system is regularly verified by _____, and at
all times pertinent to the records certified here the process and system functioned
properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of
the Federal Rules of Evidence.

Date Signature

AFFIDAVIT OF SPECIAL AGENT KLEINOSKY- 58
USAO# 2020R00187

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970